Elevated Connectivity from Secure End User Devices
INTRODUCTION

UKCloud is one of very few cloud providers that has achieved Pan Government Accreditation (PGA) and PSN Accreditation for our Elevated OFFICIAL (formerly IL3) Compute, Storage and Email cloud services. One of the key benefits of an Elevated OFFICIAL cloud service is the enhanced security it offers due to controls such as more restrictive network connections, additional vetting of end-user personnel and heavily locked down end-user devices, as described in CESG guidance. However, those additional controls also create a challenge as the locked down networks and devices used by many government customers and UKCloud partners (operating at Elevated) can make it difficult to manage assured cloud services such as UKCloud's.

A core component of the UKCloud Compute as a Service platform is VMware® vCloud Director which enables customers to control their virtual data centre, virtual machines and virtual networks. This requires a number of programmes to be installed and run on any locked-down devices used to access our platform — this in turn can sometimes cause problems depending on the specific use case. For example, in order to view remote consoles of Virtual Machines (VMs), a small Windows executable file for the VMware® Remote Control (VMRC) needs to be installed on the locked-down devices, and also a browser plug-in installed and enabled.

In addition, to upload or download VMs, a Java plug-in needs to be installed and enabled in the client browser. It has been found that for some implementations of locked-down devices, software can be installed by an administrator, however sometime later a configuration management tool will automatically remove the software.

One way of addressing the problems experienced when using locked-down devices to access our platform is to deploy and access your VMs through a Bastion Host.

This Blueprint document details how UKCloud customers can configure a Bastion Host to facilitate access to our platform via Secure End User Devices.

IN THIS BLUEPRINT

- Access via a bastion host 3
- Security considerations 4
- Connectivity from device to host 4
- About UKCloud 6
ACCESSING THE UKCLOUD PLATFORM VIA A BASTION HOST

As described in CESG guidance such as Architectural Pattern 2: Walled Garden Architecture, Bastion Hosts are used as an intermediate point of authentication and connection, perhaps in conjunction with a Remote Access VPN solution. This means that security is not compromised as there is always a managed, known clean Bastion Host between the secure Elevated OFFICIAL application and potentially unmanaged or untrusted end-user device. It also provides a practical approach to not installing and maintaining software on end-user devices. Once deployed, on successful connection to a Bastion Host, users can access other services or devices within the assured environment, subject to further (different) authentication, and also subject to configuration of suitable routing/firewalling.

In the example below, a simple three-tier web application is being deployed and will be consumed over a Government Secure Network such as GSI. UKCloud customers need to access the various components of the environment via locked-down devices, but are having difficulty installing the various components or plug-ins described previously.

To enable secure connectivity, a Bastion Host has been configured on an Access or Admin virtual network within our cloud. For this example, a Windows 2008 server is being used, with Remote Desktop Services (RDS) enabled. Users on the locked-down laptops can use the Microsoft Remote Desktop Connection applet (MSTSC) to access the Bastion Host and authenticate against that machine. Once successfully logged-on, RDP or Putty can be used to access other VMs, or devices within our cloud, via the Bastion Host. In the example shown, Putty/SSH is used to access a Linux VM running Apache.

Users will also be able to access the UKCloud Portal from the web browser on their Bastion Host. They will then be able to install and activate the VMRC and Java Plug-ins required for access on that VM for permanent use (for example, including any other software needed to administer their applications or development environment).
SECURITY CONSIDERATIONS

There are various options within our cloud to further secure the scenario discussed above.

Connectivity from a Secure End-User Device to a Bastion Host

Clearly, RDP access will be required from the Secure End-User Device to the Bastion host. For many Government organisations, RDP (port 3389) is an allowed port through the LAN and perimeter firewalls – but it is worth checking. Similarly, as a secure and trusted network, RDP should already be allowed across the GSI.

At the UKCloud end of the connection, RDP is allowed through the UKCloud managed perimeter firewalls to the customer’s virtual firewall (VMware® vShield Edge Gateway). The customer will need to configure their virtual firewall to specifically allow this connection as the platform is pre-configured to deny all access unless otherwise permitted.

In this example, a firewall rule is being created to allow RDP/3389 from any external address on the GSI to the Public GSI address the customer wants to allocate for this.

Having defined the firewall rule, the DNAT needs to be defined to allow RDP traffic to NAT between the VMware® vShield Edge Gateway and the Bastion Host.

Using a vApp Edge to further secure the Bastion server

In order to further lock down access inbound and outbound to the Bastion server, a vApp Edge can be used with the Bastion server vApp. This is a scaled-down version of a VMware® vShield Edge Gateway that provides firewall and NAT services between the Bastion VM and the Organisation network it sits on.

Figure 2. Data flows between secure end point and managed server

VMware® vCloud Director will automatically set up a DNAT to map the organisation network IP address 192.168.10.10 in the diagram to the internal IP address of the Bastion Host (192.168.2.100).
Similarly, to allow the Bastion Host to communicate with the Apache server, a firewall rule can be created.

Or, the customer could be slightly less strict and allow SSH traffic to the whole Web Tier subnet.

It's also necessary to configure the VMware® vShield Edge Gateway to allow traffic between the Access network and the Web Tier network. On the VMware® vShield Edge Gateway configure the services as follows:
UKCloud has developed a range of cloud services designed specifically for the UK public sector, to help increase efficiencies, reduce costs, significantly improve procurement times and increase transparency. Our services are easy to adopt, easy to use and easy to leave to ensure that our customers remain in complete control with minimum risk. We were one of the first G-Cloud providers to achieve Pan Government Accreditation (PGA) up to Elevated OFFICIAL, and our services continue to achieve formal UK Government accreditations which make them suitable for all data at OFFICIAL (including OFFICIAL-SENSITIVE).

UKCloud’s full offering consists of:

1. Infrastructure as a Service (IaaS) – seven offerings around Compute and Storage on demand
2. Software as a Service (SaaS) – offerings for email and collaboration
3. Platform as a Service (PaaS) – based upon Open Source Digital Application Platform and Hadoop which provides organisations the benefits of using a commodity cloud platform without the added management overheads

All of UKCloud’s UK sovereign cloud computing services are hosted in one (or both) of our highly resilient tier 3 UK data centres in Farnborough and Corsham. UKCloud services are delivered with leading technologies from UKCloud Alliance Partners: QinetiQ, VMware, Cisco, EMC and Ark Data Centres. The Cloud Alliance also provides a collaborative resource which drives innovation and technical product development, helping to continually improve UKCloud’s offering to meet the needs of the UK public sector.

UKCloud is focused on providing cloud services in a more agile, secure and cost effective manner. We strive to deliver solutions that harness technology as a way to facilitate the changes that are needed to streamline processes and reduce costs to support the UK public sector and, ultimately, UK citizens and taxpayers.

MORE INFORMATION

For further information about UKCloud and how we can help you, please send an email to info@ukcloud.com